Web Images Videos Maps News Shopping Gmail more ▼

Scholar Preferences | Sign in

Google scholar | el gamal reencryption sequential serial input | Search | Advanced Scholar Search

**Scholar** | Articles and patents | anytime | include citations | ✉ Create email alert | Results **1** - **10** of about **26**. (**0.10** sec)

Did you mean: el gamal *encryption* sequential serial input

[PDF] Prêt à Voter with Paillier Encryption-extended journal version — **[PDF]** from ncl.ac.uk

PYA Ryan - J. Math. Model. Voting Syst. Elections: Theory and Appl ..., 2008 - cs.ncl.ac.uk

... nothing, but it enables the voter, or perhaps proxies acting on her behalf, to verify that the receipt is correctly **input** into the ... A earlier version of Prêt `a Voter presented in [33] used **ElGamal** encryption, [15], and **re-encryption** mixes. ... **El- Gamal** is a randomising encryption algorithm. ...

Cited by 2 - Related articles - View as HTML - All 5 versions

Deterring voluntary trace disclosure in **re-encryption** mix-networks — **[PDF]** from psu.edu

X Wang, P Golle, M Jakobsson... - ACM Transactions on ..., 2010 - portal.acm.org

... Decryption of an **ElGamal** ciphertext (G, M) is computed by the expression M · G −x. One can **re-encrypt** a ciphertext (G, M) by choosing δ R ← Z∗ q and eval- ... Page 10. 18:10 • X. Wang et al. ... Page 11. Deterring Voluntary Trace Disclosure in **Re-encryption** Mix-Networks • 18:11 ...

Cited by 5 - Related articles - All 23 versions

[PDF] Chaum's Visual Voting Scheme without RPC — **[PDF]** from psu.edu

M Klonowski, M Kutyłowski, A Lauks... - 2008 - Citeseer

... In this paper, a method of shuffling **El-Gamal** ciphertexts is presented - after processing a whole ... First, the last server presents the **ElGamal** ciphertext from which it has obtained m, say (a, b ... Duplicating an onion: Thanks to **re-encryption** features, a duplicate can be easily hid- den. ...

Related articles - View as HTML - All 4 versions

Parallel mixing — **[PDF]** from psu.edu

P Golle, A Juels - Proceedings of the 11th ACM conference on ..., 2004 - portal.acm.org

... this paper, we consider exclusively **re- encryption** mixnets, ie mix networks that **re-encrypt input** ciphertexts and ... Our construction is applicable to any **re-encryption** mixnet whose costs are linear in the ... ful- filled by the mixnets of Furukawa and Sako [9], Neff [19], Jakobsson et al. ...

Cited by 26 - Related articles - All 35 versions

The security implications of VeriChip cloning — **[HTML]** from nih.gov

J Halamka, A Juels... - Journal of the ..., 2006 - jamia.bmjjournals.com

... If IDs are indeed assigned **sequentially** in production, for instance, then an attacker that observes the ID of one employee in a given corporation can probably guess the IDs ... **El Gamal** T. . A ... Okamoto T. Golle P,; Jakobsson M,; Juels A,; Syverson P. . Universal **re-encryption** for mixnets ...

Cited by 33 - Related articles - All 20 versions

Pr•t ā Voter with Paillier encryption

PYA Ryan - Mathematical and Computer Modelling, 2008 - Elsevier

**...** or perhaps proxies acting on her behalf, to verify that the receipt is correctly **input** into the **...** à Voter receipts into a pure ciphertext term that can be put through a **re-encryption** mix. The disadvantage of exponential **ElGamal** is that we have to constrain the plaintext space in order to **...**

Related articles

[PDF] A critical review of receipt-freeness and coercion-resistance

**[PDF]** from scialert.net

B Meng - Information Technology Journal, 2009 - scialert.net

**...** Wikström (2005) introduced the first **El-Gamal** based mix-net in which each mix-server partially decrypts and permutes its **input**, called sender verifiability, ie, no **reencryption** is necessary. **...** shuffle based on the Boneh-Goh-Nissim cryptosystem and a **re-encryption** shuffle based **...**

Cited by 1 - Related articles - All 7 versions

[PDF] ANR Project PACE

**[PDF]** from francetelecom.com

S Canard, A Gouget, FLPPH Sibert... - pace.rd.francetelecom.com

**...** 38 3.3 Proxy **re-encryption** . . . . . . **...** He presented **sequential** aggregate signature and **sequential** aggregate signed data schemes that offer numerous advantages over those of Lysyanskaya et al. **...** [8] G. Neven. Efficient **Sequential** Aggregate Signed Data. In EUROCRYPT, pp. **...**

Related articles - View as HTML - All 2 versions

[PDF] A Bibliography of Publications on Cryptography: 2000–2009

**[PDF]** from u-aizu.ac.jp

NHF Beebe - 2010 - u-aizu.ac.jp

**...** efforts [Pau02a]. Eggs [Wei05]. EGPGV [MFS+09]. Egypt [Sin00]. Eighth [ELvS01]. Einstein [MNT+00]. EJB [TEM+01]. **El-Gamal** [EKRMA01]. election [Cal00a]. electronic [AvdH00]. element [MS02a]. Elementary [Ste08]. Eleven [All03]. **ElGamal** [BJN00]. **ElGamal**-like [CWH00]. **...**

Related articles - View as HTML - All 4 versions

[PDF] Fine-tuned implementation of an efficient secure profile matching protocol

**[PDF]** from psu.edu

N Mavrogiannopoulos, LAM Schoenmakers - Citeseer

**...** Thus the expo- nentiations left are the one from Pedersen commitment and 4 exponentiations for the random **re-encryption** operations. Overall the computational complexity for exponentiations, including the **El**- Page 22. 2.5. CONDITIONAL GATE 15 **Gamal** decryption ste

Related articles - View as HTML - All 5 versions

Create email alert

Did you mean to search for: el gamal ***encryption*** sequential serial input

Gooogle ▶

Result Page: **1** 2 3 **Next**

el gamal reencryption sequential se Search

Go to Google Home - About Google - About Google Scholar